Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1708 02/20/15

~ Cyberattacks Hit Banks ~ People Are Talking! ~ HTTP 2.0 Approval
~ Lizard Squad Returns! ~ Obama: EU Can't Compete ~ Email Search Curb?
~ Twitter Under Pressure ~ Net Neutrality "Holes" ~ Onion City Search!

~ Spyware Embedded by US ~ Mark Cuban Weighs In! ~ Photoshop Hits 25!

-* Sony Banking on PlayStation! *-
-* Peter Banks on Asteroid's Direction *-
-* Hackers Still Inside U.S. State Dept Email *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Another week, another issue out late! Sorry about another delay this week, but Mother Nature continues to pound us here in the Northeast (and lots of other areas throughtout the U.S.!). We've been spending a lot of time to continue cleaning up after all of these recent snow storms, including clearing snow and ice from our roofs. What we couldn't get off of the roof, we had some contractor come in and finish it up. They weren't as successful as I would have liked removing the ice, but I'm hoping that they did enough to prevent any problems with the impending ice storm that's on its way this weekend.

So, after another week of dealing with snow, ice, and the frigid cold weather - we're tired. Didn't make it a late night last night trying to finish up here, so here we are, late.

Let's get right to this week's issue - a lot of interesting stuff for you this week!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Sony Looking to PlayStation For Profitable Future
"""""""""""""""""""""""""""""""

Lizard Squad Returns, Claims Attack!
Peter Banks on Asteroids New Direction
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Sony Looking to PlayStation For Profitable Future

Sony has revealed its plans for increased profitability in the coming years center on PlayStation and cameras, while it may depart the TV and smartphone business.

According to Reuters, CEO Kaz Hirai made the announcement explaining that the dominance of Apple and Samsung meant it was becoming increasingly nonsensical to pursue sales growth in the smartphone sector. When asked whether the TV and phone businesses could go the way of its PC arm, which was recently sold off, Hirai said he wouldn't rule it out.

As a result, the company plans to focus on entertainment, camera sensors, and the increasingly successful PlayStation business to see it return to profit. One of the key aims Hirai outlined was expanding the PlayStation Network userbase while also focusing on its music-streaming service.

Currently, Sony is forecasting its sixth net loss in seven years at the end of this financial year, though things seem to be on the turn. This aggressive restructuring coupled with the PS4's success has been applauded by investors, with shares rising 80 percent over the past year alone.

Once all this is said and done, Hirai said, he hopes to see Sony post an operating profit of at least 500 billion yen ($4.2 billion) for 2017/18, compared with the 20 billion yen forecast for the year ending March 31. If the company does manage to focus in on the success PlayStation has achieved recently while continuing to sell off less-successful investments like SOE, it could very well manage it.

Lizard Squad Returns, Claims Attack on Xbox Live and Daybreak Games

Hacking group Lizard Squad returned over the weekend with alleged fresh attacks against Microsoft's Xbox Live service and the studio formerly known as Sony Entertainment Online.

The group first targeted Sony in August when it launched a DDoS attack against the PlayStation Network (PSN).

Then, over the Christmas period, it launched similar attacks against Microsoft's Xbox Live, as well as PSN again.

In January, the tables were then turned on Lizard Squad after the hacking of its own DDoS-for-hire service LizardStresser.

And in the last two months two alleged Lizard Squad members have been arrested.

But on Saturday the group reappeared, apparently turning its attention to Daybreak Games - previously known as Sony Online Entertainment - who reported that its servers were being attacked.

The company said many of its online games, including the newly released zombie survival MMO H1Z1, were experiencing connection issues.

Daybreak Games president John Smedley explained that the game was being targeted by a DDoS attack which prompted a reply from someone using the

Squad’s hatted-lizard image, and the account handle @LizardPhoenix:

What’s up, long time no see :).@j_smedley

The group and Smedley already have some history of course - in August 2014, a bomb threat was sent to a plane on which Smedley - then the Sony Online Entertainment president - was travelling.

Since then, Sony sold Sony Online Entertainment to Columbus Nova which renamed the studio Daybreak Games.

Not content, it seems, with just disrupting Daybreak Games, the same Twitter account announced an attack against Microsoft’s gaming network on Sunday.

The group claimed responsibility for the Xbox Live outage, saying that the attack was orchestrated in association with another group called Like No Other (LNO):

XBL attack was done with the help of our associates from LNO: @LNOuNiTy @LNOVenom @Guidelines @we_are_lno

By way of celebration, Lizard Squad followed that tweet up with another which read:

Haha "Xbox" is trending Worldwide. We’re back :)

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Museum Establishes World Video Game Hall of Fame

The Strong, a collections-based museum in Rochester, New York, has established the World Video Game Hall of Fame.

The Hall of Fame will recognize games from all platforms, including arcade, console, computer, handheld, and mobile. In order to be considered for induction, a game must meet the following criteria: icon-status, longevity, geographical reach, and influence. The museum notes that if a game’s influence is strong enough, it doesn’t have to meet the first three criteria.

The Strong is currently home to the National Toy Hall of Fame, as well as the International Center for the History of Electronic Games, which contains over 55,000 video games and related artifacts.

To nominate a game, head over to The Strong’s website. Nominations will be accepted through March 31, with finalists being selected by a committee of journalists, scholars, and others familiar with video game history. The first batch of inductees will be revealed in June during a ceremony at the museum.

Atari Producer Peter Banks on Asteroids New Direction

As I listlessly skimmed my email s inbox, I was suddenly slapped awake by an interesting subject line, Atari reviving Asteroids.

I loved the sound of that idea. The original Asteroids concept of destroying space boulders, while fighting inertia, would be a great starting point for a modern shoot-em-up title.

As I dug into the email, however, it became clear that my assumptions were off by, like, a lot. Atari is rebooting the series with Asteroids: Outpost, but as an, open-world, sandbox-style survival experience.

That doesn t sound like the Asteroids I know. It probably doesn t sound like the Asteroids you know, either.

To help me wrap my head around developer Salty Games concept, Atari producer and Asteroids: Outpost s executive producer Peter Banks came to my aid.

GamesBeat: I was a bit shocked by the Asteroids: Outpost announcement earlier this week. When someone mentioned an Asteroids reboot, I did not expect it to be described as an open-world, sandbox-style survival experience. What prompted taking the gameplay in this direction?

Peter Banks: Like many of Atari s great [intellectual properties], Asteroids has a long and storied history. Since 1981, we ve seen the title appear across a number of different platforms. With the legacy of official versions and clones out in the world, you could almost call Asteroids a genre unto itself.

That said, our goal with Asteroids: Outpost is really to expand the world of Asteroids beyond a single gameplay mechanic and explore the wider context of the game. While we certainly intend to appeal to longtime fans of the franchise, we also want to open up the game to newcomers and those used to more modern gameplay conventions.

GamesBeat: Is the original Asteroids concept somewhere in Asteroids: Outpost s gameplay?

Banks: Absolutely. The game is set on a massive asteroid, in our solar system s asteroid belt, and part of the game is defending yourself and your base against deadly asteroid showers.

Tied to this, a core gameplay mechanic is the construction and control of anti-asteroid defense systems to protect your outpost. This mechanic evokes classic gameplay without specifically reproducing it and fits comfortably within the larger context of the overall gameplay.

GamesBeat: Most of the classic Atari franchises we know and love come from a time when video games were extremely young. Games like Asteroids were groundbreaking for their time, but man, they were also extremely basic and bare bones. They are to video games what the silent era is to film. How do you approach the challenge of creating a modern take on these simple game concepts?

Banks: A very good point, and this is something that s an essential component of our greenlight process.

Some of these titles have really compelling gameplay mechanics we want to focus on. Others present rich or well-loved settings we feel can be explored. In the case of Asteroids the core concepts are a satisfying destruction of asteroids and an evocative, deep space setting. We love the challenge this kind of process presents us it gives us a blank canvas to create something really compelling while at the same time providing us with this rich vein of history in which to inspire us.

GamesBeat: Why is Atari going Early Access with Asteroids: Outpost?

Banks: Early Access is an important part of a strategy that focuses on a long-term engagement with our players.

As a multiplayer-focused game, much of the core gameplay [in Outpost] will center on emergent user behaviors. While we do extensive concepting, design, and testing before even reaching Early Access, we ve really found with our own games, as well as in the games we love to play, [that] the gameplay elements that players really end up enjoying are often ones that they themselves have a hand in crafting. Early Access gives players and our developers a great way to tinker and improve on the core gameplay we ve created for Asteroids: Outpost.

GamesBeat: Do you see Early Access, and even some forms of crowdfunding, as potentially risky from a development standpoint? It seems like the incentive for finishing a game as in gaining a player base and selling a product is gained before reaching completion under these systems. Doesn t that kill some of the drive to see a project through to the end?

Banks: Developing and publishing games is an inherently risky endeavor it s a volatile market with high stakes. That said, the expectation for multiplayer today is that games will be supported over time with regular updates, new content, [and so on].

In the case of Asteroids, we are extremely excited to have a wealth of data from Early Access to further enhance and refine the gameplay for Asteroids: Outpost and continue rolling out content. Basically, it s the first step in a long-term commitment to a player-focused development strategy.

GamesBeat: There is something strange going on with recent Atari releases. I thought it was just Alone in the Dark: Illumination, but I noticed Haunted House: Cryptic Graves, Minimum, and Asteroids: Outpost are doing the same thing: They are all PC-only releases. What s going on here? These all seem like they should be major cross-platform, cross-console projects for Atari.

Banks: Atari has a long history of success in the PC market. Digital distribution has been a huge part of our strategy for years, so this in itself is nothing new. We re still relatively early in this console cycle, and the current install base only supports a fairly finite number of titles. For now, PC really fits our strategy, it allows us to be a bit more experimental and reactive.

GamesBeat: Is there anything else you can tell us about Asteroids: Outpost beyond this week s announcement?

Banks: We re just getting started! We ll have tons more to share in the coming weeks and months as we head into Early Access and beyond!

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Spyware Embedded by U.S. in Foreign Networks, Security Firm Says

The United States has found a way to permanently embed surveillance and sabotage tools in computers and networks it has targeted in Iran, Russia, Pakistan, China, Afghanistan and other countries closely watched by American intelligence agencies, according to a Russian cybersecurity firm.

In a presentation of its findings at a conference in Mexico on Monday, Kaspersky Lab, the Russian firm, said that the implants had been placed by what it called the Equation Group, which appears to be a veiled reference to the National Security Agency and its military counterpart, United States Cyber Command.

It linked the techniques to those used in Stuxnet, the computer worm that disabled about 1,000 centrifuges in Iran s nuclear enrichment program. It was later revealed that Stuxnet was part of a program code-named Olympic Games and run jointly by Israel and the United States.

Kaspersky s report said that Olympic Games had similarities to a much broader effort to infect computers well beyond those in Iran. It detected particularly high infection rates in computers in Iran, Pakistan and Russia, three countries whose nuclear programs the United States routinely monitors.

Some of the implants burrow so deep into the computer systems, Kaspersky said, that they infect the firmware, the embedded software that preps the computer s hardware before the operating system starts. It is beyond the reach of existing antivirus products and most security controls, Kaspersky reported, making it virtually impossible to wipe out.

In many cases, it also allows the American intelligence agencies to grab the encryption keys off a machine, unnoticed, and unlock scrambled contents.

Moreover, many of the tools are designed to run on computers that are disconnected from the Internet, which was the case in the computers controlling Iran s nuclear enrichment plants.

Kaspersky noted that of the more than 60 attack groups it was tracking in cyberspace, the so-called Equation Group surpasses anything known in terms of complexity and sophistication of techniques, and that has been active for almost two decades.

Kaspersky Lab was founded by Eugene Kaspersky, who studied cryptography at a high school co-sponsored by the K.G.B. and once worked for the Russian military. Its studies, including one describing a cyberattack of more than 100 banks and other financial institutions in 30 countries, are considered credible by Western experts.

The fact that security software made by Kaspersky Lab is not used by many American government agencies has made it more trusted by other governments, like those of Iran and Russia, whose systems are closely watched by United States intelligence agencies. That gives Kaspersky a front-row seat to America’s digital espionage operations.

The firm s researchers say that what makes these attacks particularly remarkable is their way of attacking the actual firmware of the computers. Only in rare cases are cybercriminals able to get into the actual guts of a machine.

Recovering from a cyberattack typically involves wiping the computer s operating system and reinstalling software, or replacing a computer s hard drive. But if the firmware gets infected, security experts say, it can turn even the most sophisticated computer into a useless piece of metal.

In the past, security experts have warned about the race to the bare metal of a machine. As security around software has increased, criminals have looked for ways to infect the actual hardware of the machine. Firmware is about the closest to the bare metal you can get a coveted position that allows the attacker not only to hide from antivirus products but also to reinfect a machine even if its hard drive is wiped.

 If the malware gets into the firmware, it is able to resurrect itself forever, Costin Raiu, a Kaspersky threat researcher, said in the report. It means that we are practically blind and cannot detect hard drives that have been infected with this malware.

The possibility of such an attack is one that math researchers at the National Institute of Standards and Technology, a branch of the Commerce Department, have long cautioned about but have very rarely seen. In an interview last year, Andrew Regenscheid, a math researcher at the institute, warned that such attacks were extremely powerful. If the firmware gets corrupted, Mr. Regenscheid said, your computer won t boot up and you can t use it. You have to replace the computer to recover from that attack.

That kind of attack also makes for a powerful encryption-cracking tool, Mr. Raiu noted, because it gives attackers the ability to capture a machine s encryption password, store it in an invisible area inside the computer s hard drive and unscramble a machine s contents.

Kaspersky s report also detailed the group s efforts to map out so-called air-gapped systems that are not connected to the Internet, including Iran s nuclear enrichment facilities, and infect them using a USB stick. To get those devices onto the machines, the report said, the attackers have in some cases intercepted them in transit.

Documents revealed by the former National Security Agency contractor Edward J. Snowden detailed the agency s plans to leap the air gaps that separate computers from the outside world, including efforts to install specialized hardware on computers being shipped to a target country. That hardware can then receive low-frequency radio waves broadcast from a

suitcase-size device that the N.S.A. has deployed around the world. At other times the air gaps have been leapt by having a spy physically install use a USB stick to infect the adversary’s computer.

Basing its estimate on the time stamps in code, the Kaspersky presentation said, the Equation Group had been infecting computers since 2001, but aggressively began ramping up their capabilities in 2008, the year that President Obama was elected, and began doubling down on digital tools to spy on adversaries of America.

While the United States has never acknowledged conducting any offensive cyberoperations, President Obama discussed the issue in general in an interview on Friday with Re/code, an online computer industry publication, describing offensive cyberweapons as being unlike traditional weapons.

This is more like basketball than football, in the sense that there s no clear line between offense and defense, said Mr. Obama, himself a basketball player. Things are going back and forth all the time.

Did NSA Plant Spyware in Computers Around World?

Did the National Security Agency plant spyware deep in the hard drives of thousands of computers used by foreign governments, banks and other surveillance targets around the world?

A new report from Russian cybersecurity firm Kaspersky Lab said its researchers identified a new family of malicious programs or worms that infected computers in multiple countries, primarily overseas. Targets appeared to be specifically selected and included military, Islamic activists, energy companies and other businesses, as well as government personnel.

Without naming the United States as the source of the malware, the report said one of the programs has elements in common with the so-called Stuxnet worm, which the New York Times and Washington Post have said was developed by the U.S. and Israeli governments to disrupt Iranian nuclear facilities. Based on their similarities, the creators of both programs "are either the same or working closely together," Kaspersky’s report said.

The malware was not designed for financial gain but to collect information through "pure cyberespionage," added Kaspersky researcher Vitaly Kamluk. In its report, the firm said the malware was extremely sophisticated and "expensive to develop."

NSA spokeswoman Vanee Vines declined comment Tuesday, but cited a 2014 presidential directive that instructed U.S. intelligence agencies to respect Americans’ privacy while continuing to conduct overseas operations necessary to guard against terrorism or other threats.

Kaspersky researchers said some of the spyware was designed to burrow into the essential software that comes pre-installed on a computer’s disk drive, known as firmware. Once there, it was difficult to detect and virtually impossible to remove, and it could gain access to vital codes, such as the keys to deciphering encrypted files. Kamluk said compromising firmware is a difficult technical challenge that likely requires knowledge of the manufacturer’s source code normally a closely guarded secret.

The report named several disk drive manufacturers whose products were compromised, including Seagate Technology, Western Digital Corp., Toshiba and IBM Corp. While some did not immediately respond to requests for comment, three companies said the report came as news to them.

"We take such threats very seriously," Western Digital spokesman Steve Shattuck said Tuesday, adding in a statement that the company is "in the process of reviewing the report from Kaspersky Labs."

Seagate Technology said it "has no specific knowledge of any allegations regarding third parties accessing our drives." The company said in a statement it's committed to security and takes steps to prevent tampering or "reverse engineering" of its products. Toshiba said it had no knowledge of the malware and declined further comment.

While some of the malware was transmitted over the Internet, Kaspersky said one worm spread through infected USB thumb drives, allowing it to collect information from computers that are "air-gapped" or disconnected from the Internet. Air-gapping is a security practice used at nuclear plants and other sensitive facilities.

Kaspersky also said it uncovered "classic spying methods" in which scientists who attended an international conference in Houston were later sent a CD of conference materials from the event's sponsor. The sponsor apparently didn't know that the disc also contained malware which spread into certain attendees' computers, the researchers said.

Kaspersky said it found signs the malware infected computers in more than 30 countries, with the heaviest concentrations in Iran, Russia, Pakistan, Afghanistan and China. There were relatively few targets in the U.S. and Britain, said Kamluk, who characterized them as individuals living or visiting in those countries rather than companies or institutions based there.

Though it's less well-known in the United States, Kaspersky is respected in the cybersecurity industry and its reports are generally viewed as reputable. While some critics have suggested the firm has close ties to Russian authorities, several experts said Tuesday that it's plausible the United States is behind the malware identified in the report.

"A lot of nation-states are involved in these activities. Russia, China and the U.S. are in a great cyberarms race," said David DeWalt, chief executive of the Silicon Valley cybersecurity firm FireEye. He noted that China has been implicated in attempts to steal source code and other information from U.S. companies, for example, while Russian authorities have been linked to some hacking efforts.

Some warned that U.S. efforts could have unintended consequences: Foreign customers could become more leery of U.S. tech products if they're suspected of being used for spying. And other hackers may be able to exploit the same vulnerabilities, said cybersecurity expert and author Bruce Schneier.

Over 100 Banks Hit by Sophisticated Cyberattack

A sophisticated global cyberattack struck more than 100 banks in 30

countries stealing hundreds of millions of dollars, The New York Times reported Saturday.

Citing a soon to be released report from computer security company Kaspersky Lab, the newspaper said the attack involved malicious software that gave hackers long-term access to banking systems.

A group of Russians, Chinese and Europeans was able to siphon off around $300 million in one of the world’s largest bank robberies, the report said.

The money was transferred to bank accounts around the world in small-value amounts to avoid detection.

Hackers largely focused on banks in Russia, but millions of dollars were also taken from banks in Japan, the Netherlands, Switzerland and the United States as well, the Times said.

Hackers had such advanced access to the banks’ systems that they could force ATM machines to dispense cash at specific times and locations where hackers could pick it up.

Hackers Still Inside U.S. State Department Emails

Both government and private security specialists are still struggling to end the hackers presence inside an unclassified section of the State Department s email system.

According to two official sources, security teams have not been able stop the hackers from accessing the email system, despite first discovering the hack around 3 months ago. The intruders are using a wide variety of changing techniques to outwit the security teams, although no classified State Department material seems to have been compromised, writes John Walcott of Bloomberg.

Despite the lack of a serious breach, officials are still worried because the presence of the hackers enables them to write false emails, delete genuine messages and continue searching for a way into classified communications systems.

One of the officials, who requested anonymity, said that a number of factors appear to suggest that the attack may be linked with Russia. One former U.S. intelligence official claims that Russia s cyber-espionage capabilities are almost on par with the U.S. National Security Agency.

The cyber intrusions come at a time of deteriorating relations between the U.S. and Russia, with the ongoing conflict in Ukraine a major source of tension.

Hackers linked to the Russian government have been known to use similar phishing techniques in the past, where victims are incited to open e-mail attachments infected with malware which then allows hackers to access email systems.

This time around the investigation has not reached any definitive conclusion on the origins of the intruders, according to the officials.

We have robust security to protect our systems and our information, and we deal successfully with thousands of attacks every day, said Marie Harf, a State Department spokeswoman. We take any possible cyber intrusion very seriously.

The persistent attacks followed a report from Moscow-based cyber security company Kaspersky Lab which claimed that tens of thousands of computers across the globe had been infected with surveillance software following a highly sophisticated spying campaign.

The Russian company stopped short of alleging that the hackers were associated with the NSA, but Costin Raiu, director of Kaspersky s global research and analysis team, did say that the sophistication of the attack would point to the involvement of government spy agencies in the U.S., Britain, Russia or China.

U.S. security teams need to get the hackers out of the State Department email system before they work out a way of causing damage or accessing classified information.

Net Neutrality Advocates Identify Holes in FCC s Net Neutrality Plan

Net neutrality advocates are generally pleased by the Federal Communications Commission’s latest plan to regulate Internet service providers, but some are pointing out potential problems.

Attorney Matt Wood, the policy director for advocacy group Free Press, told the FCC last week that it faces "legal obstacles" in how it intends to regulate Internet service providers. FCC Chairman Tom Wheeler proposes to reclassify Internet service providers as common carriers in two parts. ISPs will be common carriers in their relationships with home Internet consumers. They will also be common carriers in their business relationships with "edge providers," companies that offer services, applications, and content over the Internet.

"[B]oth the service to the end user and to the edge provider are classified under Title II [of the Communications Act]," the proposal states.

This could get the FCC in trouble, Wood argues:

On the statutory definition question, as we noted in our earlier letter, services purportedly offered to a remote edge provider when there is no physical connection between that edge provider and the carrier in question are not services offered directly to the edge provider according to any precedent we could find. If there is no physical connection, and thus no obvious direct relationship between the carrier and the remote edge provider, it is hard to imagine how the service can qualify as a telecom service under Section 153(53) of the Act. That subsection stipulates that a telecom service must be offered directly to the recipient.

Likewise, as we also noted in our letter, even in the rare case where there is a direct interconnection with an edge provider this is likely private carriage. Such arrangements are negotiated on an individual basis with the broadband provider, not offered indiscriminately on a common carrier basis to the public under the same definition in

subsection (53).

Even if the Commission could surmount these statutory barriers, the policy question remains: why would it want to? Our November 5 letter described the seemingly absurd results that could flow from recognizing such a relationship between edge providers and end-users broadband providers. Would such an approach suggest or even mandate that every single end point on the Internet is a customer of each and every ISP that provides service to any other single end point on the Internet? Put more colloquially, would every website in the world become a customer of any broadband Internet access service provider whose end-users visit that website?

The FCC could establish jurisdiction over interconnection disputes without claiming that ISPs are offering a service to edge providers, Wood argued. Money disputes between ISPs and content providers can result in poor performance for consumers, he noted this happened with Netflix on multiple ISPs for months. Net neutrality rules designed to protect Internet users should thus allow the FCC to intervene in interconnection battles that harm traffic to end users, Wood wrote.

"Broadband users deserve access to the content, services and applications of their choosing, and they deserve access to such data at the speeds for which those end-users are paying," Wood wrote. "If the Commission s rules in this proceeding are intended to prevent broadband Internet access service providers blocking, degrading or impairing the delivery of such traffic as sent and received by Internet users, then the rules should clearly prevent the imposition of such access charges even in the guise of ’interconnection fees’ along with other harmful conduct at the interconnection point with a broadband Internet access service provider s last-mile network."

The FCC’s previous net neutrality rules were thrown out in court when judges ruled that the commission imposed per se common carrier regulations without first reclassifying broadband as a common carrier service. That, plus prodding from President Obama and public support for stronger net neutrality rules, helped convince Wheeler to use Title II.

Another concern was raised in a filing by the National Association of Regulatory Utility Commissioners (NARUC).

NARUC said it supports "whatever legal rationale the Commission adopts to support imposition of net neutrality principles," meaning that the group does not object to reclassifying broadband providers as common carriers.

But NARUC wants to make sure the FCC doesn’t rule out the possibility of reclassifying Voice over Internet Protocol phone systems offered by Internet providers. The FCC has never firmly classified VoIP as either a common carrier service or not, and the FCC’s net neutrality proposal has a carve-out for VoIP.

"Some data services do not go over the public Internet, and therefore are not ’broadband Internet access’ services subject to Title II oversight (VoIP from a cable system is an example, as is a dedicated heart-monitoring service)," the proposal states.

NARUC worries that industry groups will point to this in their argument that VoIP is a lightly regulated "information service" instead of a more heavily regulated telecommunications service.

"It is true... that, however classified, both VoIP and a dedicated heart monitoring service, are not in any sense ’broadband internet access,’" NARUC wrote. "Unfortunately, an opposite inference can be drawn from the cited text."

VoIP’s classification isn’t directly related to net neutrality but will become important over the next few years as telephone companies like AT&T and Verizon shift customers from circuit switched landlines to IP voice systems. The old phones are regulated as telecommunications services under Title II, while VoIP so far has escaped strict regulation.

NARUC asked the FCC to clarify that a telecommunications service such as voice should be regulated as telecommunications regardless of what underlying technology powers it. "Failing that, the FCC should clarify the cited text to make clear that the Agency is not attempting to change the classification of VoIP services to information services," NARUC wrote.

Essentially, NARUC wants the FCC to impose common carrier rules on VoIP providers right now, or at least not prevent itself from doing so in the future.

Mark Cuban: FCC s Net Neutrality Plan Will F Everything Up

Billionaire investor and star of ABC s Shark Tank Mark Cuban thinks the Federal Communications Commission s plan to regulate the Internet as a public utility will do damage of profane proportions to the industry.

 That will fuck everything up, Cuban said at the Code/Media conference on Wednesday in California, according to re/code. Net neutrality is just a demonization of big companies.

According to Cuban, there s little evidence to support the claims that Internet service providers like Verizon, AT&T, Comcast, Time Warner Cable or others ever slowed service speeds to content creators like Netflix, Google YouTube, Amazon or others in order to force the companies into paying higher prices for acceptable service.

Such paid prioritization along with all-out content blocking would be banned under the new FCC proposal, which will classify ISPs as public utility common carriers, and regulate them in the fashion used to break up telephone monopolies at the dawn of the communication age.

Cuban along with Republican regulators, lawmakers and industry lobbyists argue the plan will destroy the market competitiveness that drives innovation and expansion to faster and larger networks, with greater choices for Internet consumers.

 Having [the FCC] overseeing the Internet scares the shit out of me, Cuban said.

Obama Accuses EU of Attacking American Tech Companies Because It ’Can’t Compete’

Barack Obama has angered officials in Europe after suggesting that investigations by the European Union into companies like Google and Facebook were "commercially driven." In an interview with Recode, the president claimed that European "service providers who can t compete with ours, are essentially trying to set up some roadblocks for our companies to operate effectively there." The truth, however, is more nuanced than this.

Obama says: "We have owned the internet. Our companies have created it, expanded it, perfected it in ways that they can t compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."

Over the past few years, it's true that EU regulators have attempted to crack down on what they perceive as the unfettered power of American companies in Europe. The targets for these officials haven't just been limited to commercial power and have included issues such as tax avoidance and privacy rights including the so-called right to be forgotten which gives EU citizens the right to petition Google to remove links from certain search results.

In response to questions concerning Silicon Valley's intrusion into people's personal data, Obama singled out Germany as a country that was "very sensitive to these issues." The president suggested that this was due to the country's "history with the Stasi" the communist secret police that terrorized East Germany following World War II. Germany's chancellor Angela Merkel has previously compared the NSA to the Stasi.

A spokesperson for the European Commission called Obama s comments "out of line," saying that "regulation should make it easier for non-EU companies to access the single market," according to a report in the Financial Times. The unnamed official said that "it is in [US companies] interest that things are enforced in a uniform manner." (The "single market" mentioned here is an ongoing plan to boost the EU s faltering economy with initiatives promoting the digital industry.)

Last year, the European Parliament voted in favor of breaking up Google There's undoubtedly a desire in Europe to curb the commercial power of US companies. Last year, the European Parliament voted in favor of breaking up Google to ensure "competitive conditions," while other firms that are leveraging technology to beat established industries have faced a backlash. Uber, for example, triggered protests across the continent last year with taxi drivers arguing that the company was taking advantage of legislative loopholes to avoid costly regulations.

What Obama failed to mention, however, is that both European and US companies have taken advantage of the EU's readiness to regulate internet firms. In 2007 Norway-based Opera filed antitrust complaints against Microsoft, with Google later tipping off EU investigators in a follow-up case that was concluded in 2013. In the same year, Microsoft and Oracle banded together with a number of companies from both Europe and the US to launch "Fairsearch" a body that lobbied extensively against Google's dominance. The complaints still continue, with a Portuguese app store named Aptoide filing antitrust claims against Google in July last year.

On Twitter, some individuals also took offense at Obama's comments for his perceived arrogance. Martha Lane Fox, an internet entrepreneur and member of the UK House of Lords, called Obama's comments "bad bad bad" before noting that the "invention of the internet [was the responsibility of] no one country."

Obama’s comments were more balanced than this, however, with his claim that American companies "have owned the internet" reflecting the fact that it is US firms that have overwhelmingly shaped how we use the internet today. But regardless of who built the internet, no one can deny the right of those who use it to question how it works.

Twitter Under Pressure To Act More Aggressively Against Terrorists

Twitter, the social media giant, is facing mounting questions from members of Congress and outside groups over the abuse of its network by Islamic State terrorists to spread propaganda and recruit foreign fighters.

An upcoming report has identified as many as 46,000 Twitter accounts that were being used by IS sympathizers during a three-month period last fall making it by far the most popular social media service for the terror group, according to J.M. Berger, who conducted the study, to be published next month by the Brookings Institution.

But in recent weeks, how Twitter as well as other social media companies such as YouTube and Facebook polices this content is emerging as a central issue in a vexing debate that pits the limits of free speech against the government s need to confront the aggressive messaging of IS and related terror groups. It is expected to be a prime topic of a social media panel scheduled today at a White House summit on countering violent extremism.

This is the way [IS] is recruiting they are getting people to leave their homelands and become fighters, said Rep. Ted Poe, R-Texas, the chair of a House foreign affairs subcommittee on terrorism, who held a recent hearing on the issue.

While acknowledging that IS propagandists use all social media platforms, Poe said there is frustration with Twitter specifically over what he views as its insufficient response to pleas to shut down clear incitements to violence.

Poe told Yahoo News that he and other members of Congress will be sending a letter to Twitter CEO Dick Costolo this week demanding that the firm take more active measures to shut down IS tweeters. We want them to treat this the same as child pornography, said Poe, noting that the firm has been far more vigilant in shutting down obscene images than it has with those containing extremist and violent content.

But Twitter officials say the criticisms are misplaced and that its policies are no different from those of other social media companies, which rely on the public to report abuses. Officials also say the critics ignore behind-the-scenes cooperation the firm has been providing to the FBI, which at times seeks to use Twitter to track and, with luck, identify IS tweeters.

Like our peer companies, we do not proactively monitor content, a Twitter spokesman said in an email. We review all reported content against our rules, which prohibit unlawful use and direct, specific threats of violence against others. Users report potential rules violations to us, we review their reports and take action if the content

violates our rules.

In part, several sources said, Twitter s problems are of its own making. Twitter is notoriously close-mouthed in how they handle suspensions and what goes on in the company, said Berger, an expert on the use of social media. We don t know who they suspend, and why. Of all the social media companies, they have been very reluctant to be involved in discussions with the government a stance he attributes to the libertarian views of the company s founders and executives.

That attitude led to tensions with White House officials when they sought to engage the company in discussions about the policing of its network, according to two sources familiar with internal deliberations on the issue.

Lisa Monaco, President Barack Obama s chief counterterrorism adviser, has privately complained that Twitter wouldn t even return [White House officials] phone calls, said one former U.S. official. They were really pissed off.

(A Twitter official declined to comment on the record. A White House official said Twitter will be sending representatives to this week s White House summit, but none of its executives are slated to speak, either on the social media panel or at any other summit-related event. They didn t see this as a good fit, said one administration official when asked about Twitter s role in the summit.)

The use and abuse of social media platforms by IS and other terror groups has been a growing issue for U.S. and other Western law enforcement and intelligence agencies. IS has developed what Matt Olsen, the former director of the National Counterterrorism Center, has described as the most sophisticated propaganda machine of any terrorist organization. The group employs a network of cyberwarriors, based in Raqqa, Syria, whose members target young people for recruitment (leveraging popular hashtags like #World Cup and #Ebola to extend its reach) and repeatedly post vile and threatening messages, including graphic images of beheadings and other executions, such as the recent burning of a Jordanian pilot.

These efforts are believed to be spearheaded in part by a notorious British hacker, Junaid Hussain, who has previously been imprisoned for hacking into former British Prime Minister Tony Blair s address book and posting personal details online.

The congressional concerns about Twitter s policies were amplified by the recent disclosure of an internal memo written by Twitter CEO Costolo taking his own firm to task for its failure to shut down tweeters who engage in cyberbullying and sexual harassment on its network. We suck at dealing with abuse and trolls on the platform, Costolo wrote in the memo. We re going to start kicking these people off right and left and making sure that when they issue their ridiculous attacks, nobody hears them.

Poe said in an interview that he wants to see Twitter take the same attitude toward IS tweeters. But even he acknowledges that the issue is complicated. In recent meetings, Poe said Twitter representatives have argued that they have taken their primary guidance from the FBI: The law enforcement agency has indicated that it often wants Twitter to leave IS-linked accounts up, so the bureau can track them.

We ll take them down when the FBI tells us to take them down, Poe said Twitter officials have argued in the meetings he has had with them. (A senior FBI official confirmed that the bureau has at times asked Twitter not to suspend accounts to help identify IS members and who they might be in communication with inside the United States.)

But former George W. Bush White House counterterrorism adviser Fran Townsend, who heads a private group called the Counter Extremism Project, which has been sharply critical of Twitter, said the FBI and U.S. intelligence agencies have plenty of other ways to track IS tweeters. The risk of recruitment and incitement to violence outweighs the benefits from surveilling them and finding out who they are, she said in an interview.

Townsend s concerns about IS tweeters are personally felt. Last fall, she reported to the FBI about menacing tweets threatening to behead her, made by one prominent IS tweeter who has used the name Mujahid Miski. (Miski has been identified in federal court papers as Mohammed Abdullah Hassan, a Somali-American who is under federal indictment on terror charges in Minneapolis and is now a fugitive. Among his recent tweets: Allahu Akbar, 5 Jews were sent to hell by two brave Muslims. Allahu Akbar, If only every Muslims could kill 1 Jew, everything would change.)

But Miski s case also shows the difficulties that Twitter and other social media firms have in cracking down on such content. Miski has boasted on Twitter that his account has been suspended 20 times; after each suspension, he slightly changes the name on his account and pops back up.

My view is that we can kick them off, but it s not going to solve the issue, said Quintan Wiktorowicz, a former White House national security adviser under Obama who specialized in countering-violent-extremism issues. It really is playing whack-a-mole.

The only long-term solution is a sustained partnership between U.S. government officials and social media companies to amplify and spread messages countering IS propaganda a major goal, administration officials say, of this week s summit.

HTTP 2.0 Wins Approval: Road to Better Encryption?

The HTTP standard is getting an overhaul and while faster Web pages are a big win for the first major revision since 1999 better encryption may have a more lasting impact.

As big data, the IoT, and social media spread their wings, they bring new challenges to information security and user privacy.

In a blog post, Mark Nottingham, chairman of the IETF working group behind creating the standards, said the HTTP 2.0 specifications have been formally approved. From here, the specs go through a request for comment phase and then published.

HTTP, or Hyptertext Transfer Protocol, is one of the standards that makes the Web tick. In a nutshell, HTTP allows a browser to connect with a Web server to load a page. HTTP 2.0 is promising faster loading speed.

As CNET noted, the HTTP 2.0 standard is based on SPDY, which was introduced by Google and adopted by other browsers. That HTTP 2.0 originated from a Google protocol has caused some consternation.

In the long run, speed is likely to be the No. 2 advance from HTTP 2.0. Encryption in HTTP 2.0 will mean fewer attacks and overall snooping. Technically, HTTP 2.0 doesn't require better encryption, but Mozilla and Google won't support the standard without it. Add it up and HTTP 2.0 will bring encryption. Anyone adopting HTTP 2.0 will need to support Transport Layer Security to interoperate with a wide range of browsers.

Nottingham noted in a blog post last year:

HTTP/2 doesn't require you to use TLS (the standard form of SSL, the Web's encryption layer), but its higher performance makes using encryption easier, since it reduces the impact on how fast your site seems.

In fact, many people believe that the only safe way to deploy the new protocol on the "open" Internet is to use encryption; Firefox and Chrome have said that they'll only support HTTP/2 using TLS.

They have two reasons for this. One is that deploying a new version of HTTP across the Internet is hard, because a lot of "middleboxes" like proxies and firewalls assume that HTTP/1 won't ever change, and they can introduce interoperability and even security problems if they try to interpret a HTTP/2 connection.

The other is that the Web is an increasingly dangerous place, and using more encryption is one way to mitigate a number of threats. By using HTTP/2 as a carrot for sites to use TLS, they're hoping that the overall security of the Web will improve.

Congress Unites To Back Law That Would Curb Warrantless Email Searches

More than half of the US House of Representatives have backed a proposed law that aims to end warrantless searches of email inboxes.

The proposed law, titled the Email Privacy Act 2015, aims to close a loophole introduced in law three decades ago, which allows the government to access and read emails that were opened more than six months earlier without a court's approval.

Rep. James Sensenbrenner (R-WI, 5th), who authored the controversial Patriot Act, and Rep. Thomas Massie (R-KY, 4th), whose election was won on supporting privacy matters, are among the 240 members of the House who co-sponsored the bill.

A corresponding bill, co-sponsored by Sen. Patrick Leahy (D-VT), was introduced in the Senate last week.

Overwhelming bipartisan support for any bill is rare. But in the wake of the National Security Agency surveillance leaks there has been a greater effort to reform the laws that allow the US government unfettered access data on US citizens, despite search and seizure protections laid out by the Fourth Amendment.

Both bills were originally introduced in 2013, but stalled in a fractious and bureaucratic session despite passing the various congressional committees. The reintroduced bills will remain in committee stage until they are voted on later this month or early next.

The proposed law aims to fix the outdated Electronic Communications Privacy Act, which is still in effect despite falling behind the curve of the digital age.
"In the nearly three decades since ECPA became law, technology has advanced rapidly and beyond the imagination of anyone living in 1986," Leahy said in a statement last week.

In this day and age when most web-based email inboxes offer free and almost unlimited storage, most historical and archived email is not deleted. That means emails that were opened and left on the server - most Gmail, Outlook, and Yahoo emails are never deleted - for more than six months can be accessed without a court order or a warrant, the Electronic Frontier Foundation says.

Email less than six-months-old still requires a warrant to be accessed.

Technology titans, including Apple, Google, and Yahoo have come forward in favor of the proposed law.

A number of privacy groups, including the American Civil Liberties Union and the Center for Democracy & Technology, also support the reform effort.

Onion.city - A Search Engine Bringing The Dark Web Into The Light

The Dark Web is reflecting a little more light these days.

On Monday I wrote about Memex, DARPA’s Deep Web search engine. Memex is a sophisticated tool set that has been in the hands of a few select law enforcement agencies for a year now, but it isn’t available to regular users like you and me.

There is another search engine that is though.

Just a few days before I wrote that article, on 11 February, user Virgil Griffith went onto the Tor-talk mailing list and announced Onion City, a Dark Web search engine for the rest of us.

The search engine delves into the anonymous Tor network, finds .onion sites and makes them available to regular users on the ordinary World Wide Web.

Up to now the best way to search for .onion sites has been to get on the Tor network using something like the Tor browser, but Onion City effectively does that bit for you so you can search from the comfort of your favourite, insecure web browser.

The site can do this because it’s a Tor2web proxy - a bit of software that acts as a go-between for the regular web and the Tor network.

It acts as a Tor client inside the Tor network and presents the sites it finds as regular web pages using subdomains of .onion.city.

One of the consequences of working this way is that Onion City search results are just regular web pages like any other, which makes them visible to you, me, the Onion City search engine and also, for the first time, Google.

In fact, Onion City's search functionality is a Google Custom Search, so if you can find something on Onion City you should be able to find it on Google too.

At the time of writing, there are about 650,000 Dark Web pages that have found their way into the regular Google index via Onion City.

Of course - as any small business owner can tell you - just because Google knows a website exists doesn't mean the site's pages will rank well. But those pages are at least in the mix now, enjoying their first rays of sunshine.

I took a quick look around and, because this is the Dark Web, I searched for amphetamines, 9mm ammunition and hackers for hire, and yes, it's all in there.?If you're tempted to do the same, I encourage you to read the rest of the article before you start.

Onion City isn't doing anything wrong and it's not 'outing' anyone on the Dark Web, it's just providing a means for regular web users to search things they would otherwise have to work a little harder to find.

It reduces the barriers between people who want to find or consume something and people who want to provide it in a way that's untraceable.

Any sites that don't want to be indexed by Onion City can exclude themselves from the index in the same way that regular sites exclude themselves from regular search engines, using a humble robots.txt file (although that does mean they appear in a public list of sites that don't want to be indexed).

Onion City users would be foolish to use it for anything illegal though because users get no protection whatsoever.

If you want to browse the Dark Web without leaving a trail, Onion City can't help - you still need to be on the Tor network using a Tor browser.

This is a Tor2Web proxy so the Tor part where the .onion sites reside is as secure as Tor and the web part where you and I reside is as insecure as the web (it isn't even available over HTTPS yet.)

What we users get is convenience, nothing more.

If you're wondering why that would be useful, just think about sites like Wikileaks.

Wikileaks is a clearing house for materials provided by whistleblowers. Up to now it has had to choose between being vulnerable and public or safe and difficult to find (a situation that's resulted in it taking out some bizarre protection.)

With Onion City, Wikileaks would have the option to retreat into the safety of the Tor network without sacrificing visibility.

Like all frontiers the Dark Web is lawless, exciting, disorganised and potentially dangerous. Frontiers don't last though; people move in, the law moves in and basic utilities are established.

Thanks to Onion City, the cyber-frontier now has it's first set of street lights.

Over 5 Million Raspberry Pis Have Been Sold

How big of a phenomenon is the Raspberry Pi? The charity organization behind the tiny, low-cost computer announced this morning that over 5 million Pis have now been sold. The original Pi went on sale about three years ago next week, so 5 million is a pretty huge milestone to hit in that short period of time. The organization boasts that this figure appears to make it "the biggest selling UK computer manufacturer ever," though you wouldn't be wrong to take issue with its comparison: Pi is selling $20 to $35 computers not machines that you're going to use for serious productivity for a few years.

Still, that's not a knock on any of the Pis. They're surprisingly capable machines at just $35, especially following the introduction of a faster new model and the addition of powerful software to run on it. The Pi is a great tool for small experiments, coding, and introducing computers to classrooms that otherwise couldn't afford them. The Raspberry Pi Foundation tells us that it estimates there's been an even split between the computers ending up in educational, hobbyist, and industrial settings. Those are encouraging figures, as the hope has always been that Pis will be used to get kids interested in computers and coding and not just end up on the shelves of existing hobbyists.

The original Raspberry Pi, known as the Model B, accounts for most of the 5 million total sales, with the foundation estimating that there are now about 3 million out there. There are about 1.5 million of the Model B+, which is an incremental successor that debuted last July, and about 100,000 to 150,000 of the Model A and Model A+ units, which are the lower-end Pi units. Finally, the foundation says there have been about 500,000 sales of the Pi 2 so far. That's a pretty good start for a computer that was announced two weeks ago.

How 25 Years of Photoshop Changed The Way We See Reality

There could be no better commemoration of Photoshop's 25th anniversary than the trove of unretouched BeyoncØ photos that leaked online Wednesday.

The photos appeared on a fan site called BeyoncØ World on Wednesday morning. Within an hour, BeyoncØ World had pulled them down, apparently alarmed at fans' genuine outrage. These fans were angry not that BeyoncØ had been Photoshopped so dramatically as is often the case with these things but that someone had dared expose her for who she actually is. Laugh lines. Blemishes. Bits of friz. All the makings of a real, human person.

The problem is that 25 years after Photoshop launched, we'd much prefer manipulations of reality to reality itself.

This isn’t entirely the fault of Photoshop, of course. While the name of the program has become synonymous with photo editing of any sort, photos were edited long, long before Adobe went to market and arguably, people have "edited" their appearance, via cosmetics and corsets and other means, since even earlier than that.

But Photoshop made such editing easy. Mainstream, even. (A review of the "idiotproof" consumer version, from 1995: "if you own a digital camera or a scanner, you can now do your own photo retouching!")

The first version of the software, released in 1990, allowed basic edits like stretching and skewing and smudging and blurring. The second version improved on things like color handling. By the sixth version, Photoshop could "heal" blemishes, layer pieces of different images on top of each other, and "liquify" the whole thing, the better to smooth out bulky forearms or too-wide waists.

Before long, "Photoshop" referred not only to a piece of software, but to a constellation of social evils, most of them visited on women: the pressure to be beautiful and unblemished and thin, the media’s complicity in this campaign, the plummeting self-esteems of girls and young women who grew up believing they should look that fake, Photoshopped way.

Faith Hill whittled to nothing on the cover of Redbook. Kate Winslet with yards-long legs in the British version of GQ. Julia Roberts’s Lancome campaign banned in Britain, over concerns that it didn’t "reflect reality."

Just last month, a high school student made waves when she published copies of her yearbook pictures, which were edited by the photographer to make her appear thinner.

"I was outraged!" The girl wrote on Reddit. "When we go and have our photos taken we are flat out told that our skin will be retouched to hide blemishes. We are not told, however, that more drastic changes are (also) made."

It seems appropriate, in hindsight, that the first photo ever Photoshopped was a picture of a faceless, topless woman, sunning herself at the beach. She was "the last woman," Gordon Comstock wrote, "to inhabit a world where the camera never lied."

Now the question is: Do cameras ever tell the truth?

After all, photo-editing has evolved far beyond Photoshop; Adobe, at this point, is for magazines and advertisers and other professionals, the people charged with giving BeyoncØ’s face that otherworldly, poreless glow. For your average smartphone-carrier, there are lower-budget tools: Instagram filters, selfie-enhancing apps, any number of free online tools. Every major social network has built photo-editing features into its app, the better to let users "touch up" the look of their lives.

"It is (so easy) to believe in a distorted reality," explains Zilla van der Born, the artist who faked a trip through Asia with photo-editing. "I wanted to make people more aware that the images we see are manipulated, and that it’s not only the models in the magazines, but also our friends on social media who contribute to this fake reality ... Together we create some sort of ideal world online which reality can no longer meet."

It’s worth remembering however, despite appearances, that perfection and reality are not the same thing. No matter how much it galls the Beyhive, BeyoncØ’s still human, and only human complete with bumps and pores and tired eyes.

Get Ready For The Internet-enabled, Speech Recognizing, Joke-telling Barbie

Oh, boy, an internet-enabled Barbie doll that uses speech recognition to talk to little kids!

Sounds interesting! What could possibly go wrong!

The BBC reports that a prototype of this joke-telling, story-swapping, interactive game-playing toy was introduced at the New York Toy Fair on Saturday.

Valentine’s Day, of course!

I, like what Barbie maker Mattel says are "girls around the world", desperately want to talk to a plastic doll, in a far more meaningful and bi-directional way than ever.

So I immediately hopped online to do a search for a video that would give me a preview.

What popped up first was, well, not the "Hello Barbie" doll herself, but the "Come On Barbie, Let’s Go Party" song. If you’ve never heard it, it features really nice lyrics about partying with Barbie, and touching her everywhere, and... hang on one minute...

Kiss me here, touch me there, hanky panky!

...wait just one minute.... hanky panky?! Touching? Touching WHERE!?

Oh dear no, we don’t want any talk of touching or hanky panky with a Wi-Fi-enabled toy, yikes!

That gives me flashbacks to the horrific stalker child predator lurking behind that demon feline Talking Angela, the smartphone app with the talking cat, behind whose eyes you could see a guy in a room! Snapping pictures of kids!!

The lurking paedophile who supposedly defied the laws of physics to show up in an animated cat’s eyeballs over the internet was, of course, just an extremely widespread, notably spittle-flecked hoax.

Will Hello Barbie likewise spark FULL CAP DIRE MISPELT WARNINGS TO STAY AWAY FROM CREEPS TALKING 2 YR KIDS THRU HIR DOLL?!

Could be. Wouldn’t be terribly surprising.

But beyond baseless hoax mongering that could scare people away from a perfectly innocent doll - one with software that’s upgraded over Wi-Fi and will at some point be giving your kids career advice, learning as it interacts, much like Apple’s digital helper Siri or Microsoft’s virtual assistant Cortana - there does, in fact, lie the potential for

actual hacking.

The thing is, internet-enabled toys are just about as safe from hacking as internet anything.

We've already seen proof that such toys are vulnerable. As the BBC reports, the Vivid Toy group released Cayla, a doll that uses speech-recognition and Google's translation tools, in November.

By January, security researcher Ken Munro had discovered a vulnerability in the doll's software that allowed for it to be compromised and programmed to say anything, including things that you certainly wouldn't want your children to hear.

In fact, The Mirror got Munro to make Cayla quote Hannibal Lecter and lines from "50 Shades Of Grey."

Munro warned that if a Cayla owner's phone is off or out of range, any device could effectively connect with the doll via Bluetooth and therefore communicate with your child.

We don't want to hear Hello Barbie giggling about fava beans and a nice Chianti. Let's hope Mattel locks her down with better security than Cayla got.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.